Appendix TOM

Description of the Technical and Organizational Measures Pursuant to Art. 32 GDPR

1 Pseudonymization and encryption of personal data (Art. 32 (1) lit. a GDPR)

1.1 Pseudonymization

Measures for processing personal data in a way that the personal data cannot be associated with a specific data subject without using additional information, provided that this additional information is kept separately and is subject to technical and organizational measures

Personal data are pseudonymized for processing insofar as this is requested by the Client.

Roles authorized to manage the pseudonymization, to implement the pseudonymization, and, if necessary, the de-pseudonymization have been defined.

Pseudonymization may take place by encrypting or removing all personal data for certain types of processing. The requirements are coordinated between the Client and the provider prior to the implementation.

1.2 Encryption

Use of procedures and algorithms that transform the content of personal data into an illegible form by means of digital or electronic codes or keys. This can be done by means of symmetric and asymmetric encryption technologies.

For the purpose of the commissioned data processing, the Client alone decides which encryption is to be used for his processing, and when; for example, this could be data at transport, data at rest, or end to end.

Remote access takes place via a VPN (Virtual Private Network) connection or in encrypted form to the terminal server.

Mobile storage media do not contain any personal data and are always encrypted for company and business documents.

Encryption takes place in line with the state of the art.

Access to or use of content only takes place within the scope of the commissioned processing and according to the Client's instructions.

2 Confidentiality (Art. 32 (1) lit. b GDPR)

2.1 Physical Access Control

Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used

The premises on which the provider's data centers are located are subject to strict security regulations.

These building sections are subject to security measures such as patrolling guards, intrusion detection systems, and camera surveillance of the internal and external doors of the data centers around the clock.

Various security zones are defined in the buildings, e.g. the control room, server areas, Client segments, data archive.

An access authorization system ensures that only authorized persons are granted access through various independent access systems. Moreover, access controls ensure authorized-only access for employees of the company. Access to individual production areas and the business area is restricted by means of secure access control systems, e.g. with magnetic cards or mechanical locking mechanisms (e.g. door locks). The handout of keys is documented in a key book.

Visitors or external service providers are only permitted to access the individual production areas when accompanied by authorized staff.

2.2 System access control

Measures to prevent unauthorized use of data processing systems

All systems and applications require authentication to use the services.

Access to the processing systems takes place with a unique personal user ID and a password.

The following minimum requirements for the password quality are met: Minimum length of 8 characters consisting of uppercase and lowercase letters, numerals, and special characters, automatic blocking if the wrong password is entered repeatedly, password renewal upon expiry of the maximum validity, trivial password check.

The employees go through a starter/changer/leaver process. Here, the responsible managers grant authorization on the basis of the "least privilege" principle to ensure user control.

System administrators and normal users are assigned separate user accounts. For privileged rights, the authorization is regularly verified.

To avoid risks, two-factor authentication methods are used for remote access.

To protect all networks against access from the outside, the access is regulated by firewalls and, by default, takes place via a security infrastructure chain comprising a proxy, virus scanner, and firewall.

Moreover, fixed regulations exist for the access to IT systems.

The login and logout actions of the users on the IT systems are logged.

When leaving the workstation, it must be locked or shut down; automatic locking after a maximum of 10 minutes has been implemented.

Additionally, an access authorization concept exists. As a general rule, all authorizations are withdrawn and must be granted explicitly. The access authorization concept is based on the principle of user roles and profiles. Personalized authorizations are granted only by the responsible departments.

Excerpts and summaries of the respective regulations can be made available on request.

2.3 Data access control

Measures to ensure that persons authorized to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified, or removed without authorization in the course of processing or use and after storage

An authorization concept exists for the access to the IT systems.

Access rights are duly documented, granted, withdrawn, and deleted as soon as an employee's activity changes.

Access rights are granted according to the need-to-know principle. Only the access rights required for the performance of the tasks are granted. The authorized manager is responsible for complying with the need-to-know principle.

The access control is based on a role-based authorization concept for system access and administration rights graded according to the fields of duty. As a matter of principle, all administrative activities are logged on the systems and can thus be traced and verified.

When access is set up for a user, the user is merely granted minimum standard authorizations. These may only be expanded by way of defined application routes, subject to the approval of the responsible supervisors/managers in order to comply with due functional separation in the authorization process (double-checking principle).

Remote access takes place via a VPN (Virtual Private Network) connection or in encrypted form to the terminal server.

Only authorized storage media shall be used. The storage of personal data of the Client on mobile storage media is only permitted by instruction of the Client.

Relevant concepts and process documentation can be made available on request.

2.4 Transmission control

Measures to ensure that personal data are not read, copied, changed, or removed by unauthorized parties while being transported or saved onto storage devices and to ensure that the planned location of personal data transfer can be checked and determined

To minimize the risk for the data subject, the employees shall be instructed to use only secure data transmission routes.

The possible data transmission can take place over trustworthy lines and networks that cannot easily be intercepted.

Data transmissions take place in the secure network (e.g. with encryption). The electronic transmission of data on public routes or over public networks is always encrypted.

Various options such as the use of SSL certificates for encrypted web communication, SSL VPN for secure connection (secure remote access), electronic signature, logging will be implemented at the request of the Client.

For the purpose of the order data processing, the Client alone decides which data are to be transmitted and which transmission paths and transmission type are to be used. Additionally, the network segments can be segregated from each other by means of access control lists, and the entire network can be secured by multi-level firewall systems. If a data line that is not trustworthy needs to be used for a transmission, the transmission can also be encrypted (e.g. via VPN, TLS, etc.).

Transmission control can be ensured by means of commissioned logging to check where personal data were or are transmitted or made available, with the help of data transmission systems.

The data backups are stored in a secure area.

To ensure transport control, storage media are only transported or shipped if this has been requested by the Client. The transport route, too, is determined by the Client. This is subject to a control and documentation process.

If storage media and confidential documents need to be destroyed, this is handled by a specialized, certified company according to DIN 66399. Until the destruction, the storage media are kept in a secure area and are protected from unauthorized access. The destruction of storage media of the controller and the logging of this destruction always take place according to the order and as instructed.

Rules of conduct exist for the use of mobile storage media (USB stick, CD, DVD, etc.). These rules ensure that no personal data are stored on mobile storage media. Any business and operational data stored on mobile data carriers are always encrypted.

Relevant concepts and process documentation can be made available on request.

2.5 Separation Control

Measures to ensure that data collected for different purposes can be processed separately

The data are separated according to the Client's instruction.

Examples of logical or physical separate at Client and/or data level: Functional separation of production/integration/test systems, use of different databases, use of access control

software and setup of access rights (including logging), different types of encryption for individual data records, logical separation (e.g. on shared systems), physical separation (e.g. on dedicated systems), etc.

Access by users that is not in line with the access authorizations is effectively prevented by means of an authorization concept.

Relevant concepts and process documentation can be made available on request.

3 Integrity (Art. 32 (1) lit. b GDPR)

3.1 Input Control

Measures to retroactively check and determine whether and by whom personal data in data processing systems has been entered, changed, or removed

The input control, as well as the period for which the resulting data are retained, are governed by the Client's instructions for his data and on his infrastructure or in his applications.

Optional logging and audit-proof filing of the logs are possible on request and must be defined. Administrative access to the systems can usually be traced by means of standard logging at the operating system level.

Where the input, alteration, and deletion of the data takes place on IT systems, the changes to these data are logged with the help of suitable logging and log analysis systems (e.g. access ID, access time, authorization, and activity).

The input control is analyzed if necessary within the scope of the instruction through manual or automated log analysis.

Relevant concepts and process documentation can be made available on request.

3.2 Organizational and technical protection of authorizations, logging measures, log analyses/audit, etc.

Further information on the protection of authorizations is documented in detail in the chapters "System Access Control" and "Data Access Control". Log analyses must be requested within the framework of the instruction and will be performed in this scope.

4 Availability and resilience (Art. 32 (1) lit. b GDPR)

4.1 Availability Control

Measures to ensure that personal data are protected against accidental loss or destruction

All facilities of the commissioned data center are physically protected against security threats and environmental dangers.

The following options can be implemented on request: Redundant power supply, HA power supply (secured by UPS) with static transfer switches (STS), diesel gensets for emergency power supply, HA air-conditioning, fire alarm systems with early fire detection and direct notification of the local firefighters, separate fire zones for each data center, intrusion detection system with door opening control, emergency concepts and plans, redundant network connections and network infrastructure, clustered systems, or redundant hardware (from components to entire servers – geo-redundancy).

All security facilities are regularly reviewed for operational and technical reliability.

Depending on the earmarking of the respective processing, various archiving options are available for a full backup, such as regular automatically initiated and monitored backups (e.g. one full backup per calendar week and daily incremental backups). The normal retention period for these backups is as instructed. The backup may take place on a separate backup system that is based in a different fire zone or a different location than the productive system.

All employees have been instructed not to store any work-related data on workstations, but to use the backup-protected file server shares set up for this purpose.

Virus protection is used on all workstations. The existence of virus production, the regular update of virus patterns, and the timely installation of security updates for the utilized operating systems and application programs are guaranteed.

Topics related to BCM (business continuity management) shall be described in detail in an incident response management concept.

Excerpts and summaries of the respective concepts on the corresponding procedures can be made available on request.

4.2 Job Control

Measures to ensure that personal data processed in the order can only be processed according to the Client's instructions

The provider has appointed an internal data protection officer. By means of its data protection organization, it ensures his due and effective involvement in relevant operational processes.

Employees are instructed about their roles and responsibilities, e.g. by way of preparatory training sessions. The provider has appointed one or several officers to control and monitor the compliance with data security requirements.

The data will only be processed according to the Client's instructions. These instructions must at least be given in text form and only by authorized persons of the Client to authorized persons of the provider.

All employees are under the obligation to maintain confidentiality and, in the case of relevant processing, to comply with special obligations such as the privacy of telecommunications and social privacy. Inspections are performed for the purpose of conducting sample audits.

Inspections of the processing sites, audits, and documentation checks shall be conducted by the Client and be supported by the provider.

Documents are kept and reviewed concerning the data protection and data security, responsibilities, and relevant procedures. The Client can inspect these documents within the scope of an audit.

Suitable contracts are concluded with external service providers in order to impose the data protection level of this agreement.

5 Process for regular testing, assessment, and evaluation (Art. 32 (1) lit. d GDPR; Art. 25 (1) GDPR)

5.1 Data Protection Management

For all areas in which personal data or special categories of personal data pursuant to Art. 9 GDPR or personal data relating to criminal convictions and offenses pursuant to Art. 10 GDPR are processed, an external data protection officer has been appointed. The data protection officer has been communicated to the Client and can be contacted whenever necessary.

In the event of a data breach, a notification shall without delay be sent to the e-mail address Datenschutz@arvato-systems.de with the necessary information as required by the legislator.

Internal audits shall regularly be conducted in order to check, assess, and evaluate the effectiveness of the aforementioned measures. The Client may conduct an audit for inspection purposes.

The assurance of a procedure for the regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures and of the security of the processing takes place via the following PDCA cycle: Plan (development of a security concept), Do (introduce TOM), Check (monitor the effectiveness / completeness), and Act (continuous improvement) by the provider.

Personal data will only be transmitted to a third country upon written approval of the Client and under consideration of standard data protection clauses.

In his own sphere of responsibility, any sub-contractor guarantees data protection management at a comparable level as the provider.

5.2 Incident Response Management

Measures to quickly restore the availability of personal data and access to these after a physical or technical incident

Business operations are ensured in the event of an emergency or major malfunction, and quick recovery of all services and processing on behalf of the Client is ensured and tested by means of regular recovery drills.

Measures to ensure the resilience of the systems and services have been arranged in such a way that even processing load peaks or continually high loads can be handled. Subjects related to the storage, access, and line capacities as well as on backup and redundancy concepts have been included in detail in the availability control.

5.3 Data Protection by Design and by Default (Art. 25 (2) GDPR)

The requirements of data protection by design and by default are implemented for all products.